14. 2007 Global Security Survey, доступен на http://www.deloitte.com/dtt/cda/doc/content/dtt_gfsi_GlobalSecuritySurvey_20070901.pdf и http://www.deloitte.com/dtt/press_release/0,1014,sid%253D1000%2526cid%253D171269,00.html
15. Global State of Information Security Survey 2007, доступен на http://www.pwc.com/extweb/pwcpublications.nsf/docid/114E0DE67DE6965385257341005AED7B
16. Insider Threat Research, доступен на http://www.cert.org/insider_threat/
17. Anderson R., Moore T. The Economics of Information Security, доступен на http://www.cl.cam.ac.uk/~rja14/Papers/toulouse-summary.pdf
18. EDUCASE: Current Issues Survey Report, 2007, доступен на http://www.educause.edu/ir/library/pdf/EQM0723.pdf

Усков А.В.

ВЫСОКОЭФФЕКТИВНЫЕ IPSEC VPN-РЕШЕНИЯ ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ ОБРАЗОВАТЕЛЬНЫХ СЕТЕЙ

uskov@insightbb.com
Государственный НИИ информационных технологий и телекоммуникаций
г. Москва

Вступление.

Радикальным способом устранения уязвимостей в корпоративных образовательных сетях (КОС), основанных на использовании IP-сетей, является создание системы защиты на третьем или сетевом уровне модели OSI (таблица 1) в связи с тем, что именно сетевой уровень IP-сетей обладает наибольшей гомогенностью [1]. Поэтому, независимо от а) использования протоколов вышележащих уровней, б) физической среды передачи данных, в) конкретной технологии канального уровня, транспортировка данных по IP-сети не может быть произведена в обход IP-протокола. Размещение средств защиты на этом уровне делает их прозрачными как для сетевых приложений, так и для пользователей сети. Дополнительно, 1) на сетевом уровне существует возможность достаточно надежной реализации защиты траффика в сети управления ключами, поскольку именно на сетевом уровне выполняется маршрутизация пакетов сообщений; 2) используемый стек протоколов IPSec обеспечивает аутентичность участников обмена данными, целостность передаваемых данных и их конфиденциальность, туннелирование трафика, шифрование IP-пакетов; 3) стек протоколов IPSec совместим как с действующей сегодня версией протокола IPv4, так и с новейшей версией IPv6, которая постепенно внедряется в сеть Интернет [2].

Таблица 1.
Уровни OSI модели,
протоколы защиты и передачи данных

Уровни модели OSI и их основное назначение		Протоколы, направленные на защиту данных	Некоторые популярные протоколы, используемые для передачи данных (указанные списки не являются исчерпывающими)	Уровень детализации данных
7	Прикладной	RADIUS, TACACS, CHAP, PAP, SSH	HTTP, Telnet, DNS, SMTP, SNMP, FTP, IRC, AIM, NFS, NNTP, NTP, SNTP, X.400, X.500, LDAP, IMAP, POP3, SMB	Данные
6	Представления и кодирования		ASN.1, XML-RPC, TDI, XDR, SNMP, FTP, Telnet, SMTP, NCP, AFP, ICA	
5	Сеансовый	SSL, TLS, SOCKS, SSH	ASP, ADSP, DLC, Named Pipes, NBT, NetBIOS, RPC	
4	Транспортный		TCP, UDP, NBP, RTMP, SMB, SPX, SCTP, DCCP, RTP	Блоки
3	Сетевой	Стек протоколов IPSec (IKE, AH, ESP)	IP, IPv6, ICMP, IGMP, IPX, DDP, ARP, RARP, DHCP, BOOTP, SKIP, RIP	Пакеты
2	Канальный	L2F, L2TP, PPTP	STP, ATM, SLIP, Ethernet, FDDI, Frame Relay, Token ring, PPP, PPPoE	Фреймы (кадры)
1	Физический		RS-232, RS-422, RS-423, RS-449, RS-485, ITU-T, xDSL, ISDN (T1, E1), Ethernet (10BASE-T, 10BASE2, 10BASE5), Fast Ethernet (100BASE-T, 100BASE-TX, 100BASE-T4, 100BASE-FX), Gigabit Ethernet (1000BASE-T, 1000BASE-TX, 1000BASE-SX)	Биты

В работе [3] предложена общая модель построения систем защиты информации (СЗИ) на основе виртуальных защищенных частных сетей Virtual Private Networks – СЗИ-VPN. Основанная на ней обобщенная методика позволяет создавать частные практические решения СЗИ-VPN с использованием базовых элементов следующих множеств: *AP* – множество архитектурных решений построения сетей VPN, *TP* – множество технических решений реализации сетей VPN, *CP* – множество схемных решений сетей VPN, *P* – множество протоколов, используемых сетей VPN, *AA* – множество алгоритмов аутентификации, *PAR* - множество параметров используемых протоколов, *AC* – множество алгоритмов шифрования, *АК* – множество алгоритмов управления ключами и согласования параметров, *БД* – множество баз данных, *AC-S* - симметричные алгоритмы шифрования с закрытым ключом, *AC-P* - асимметричные алгоритмы шифрования с открытым ключом, *AC-D* - алгоритмы цифровой подписи, *AC-H* -

алгоритмы на базе функций хэширования, *AC-X* - алгоритмы распределения ключей.

Ниже рассматриваются некоторые частные методики, сформированные на основе обобщенной методики СЗИ-VPN [3], которые используют сетевой (третий) уровень модели взаимодействия открытых систем OSI; поэтому, они будут называться методиками генерации IPSec VPN-решений для СЗИ-VPN.

Методика СЗИ-VPN типа «хост-хост» для удаленного пользователя

Детальное описание данной методики, которая включает в себя следующие этапы, шаги и возможные опции, приведено в Таблице 2.

Таблица 2.

Этапы, шаги и опции методики СЗИ-VPN для VPN с удаленным доступом [3]

№ шага	Цель шага	Возможные опции или выполняемые операции
Этап 1: Схемное решение для СЗИ-VPN		
1.1.	Определить схемное решение для СЗИ-VPN	1. Строить VPN по схеме типа «хост-N –хост-M» 2. Строить VPN по схеме типа «шлюз-N –шлюз-M» 3. Строить VPN по схеме типа «хост-N –шлюз-M» Строить VPN на основе интегрирования схемных решений, где N или M могут принимать значения 1=Windows, 2=UNIX/Linux, 3=Mac, 4=CISCO IOS (для шлюзов)
(Ниже предполагается, что этапе 1 выбрано возможное решение № 1, т.е. «хост-1 – хост-1» или «хост-1 – хост-2»)		
Этап 2: Техническое решение для СЗИ-VPN		
2.1.	Определить техническое решение для СЗИ-VPN	1. Строить сеть VPN на основе программного обеспечения 2. Строить сеть VPN на основе маршрутизаторов 3. Строить сеть VPN на основе межсетевых экранов (МЭ) или брандмауэров 4. Строить сеть VPN на основе специализированных программно-аппаратных устройств 5. Строить сеть VPN на основе комбинирования нескольких вышеуказанных частных технических решений
(Ниже предполагается, что этапе 2 выбрано возможное решение № 1, т.е. «на основе ПО»)		
Этап 3: Уровневое решение для СЗИ-VPN		
3.1.	Определить уровневое решение для СЗИ-VPN (т.е. выбрать протоколы защиты передаваемых данных – см. Табл. 1)	1. Использовать защиту данных в сети VPN на основе средств канального уровня модели OSI 2. Использовать защиту данных в сети VPN на основе средств сетевого уровня модели OSI 3. Использовать защиту данных в сети VPN на основе средств сеансового уровня модели OSI 4. Использовать комбинированное решение с одновременной защитой данных на нескольких уровнях

(Ниже предполагается, что этапе 3 выбрано возможное решение № 2, т.е. стек протоколов IPSec)		
Этап 4: Подготовка к процессу аутентификации участвующих сторон (участников) сети VPN.		
4.1.	Выбрать базовый способ для аутентификации всех участников обмена данными	1. Использовать технологию цифровой подписи и цифровых сертификатов стандарта X.509 2. Использовать технологию разделяемого секрета 3. Использовать технологию активной директории и систему Kerberos
Этап 5: Создание органов сертификации в сети VPN (если на этапе 4 выбрано решение № 1)		
5.1.	Создать центральный орган сертификации	1. Использовать пакет программ «Центр сертификации» компании Microsoft (для операционных систем семейства Windows); 2. Использовать пакет программ «OpenSSL» (для операционных систем UNIX, Linux и Windows).
5.2.	Создать орган сертификации по выдаче цифровых сертификатов	1. Использовать пакет программ «Центр сертификации» компании Microsoft (для операционных систем Windows); 2. Использовать пакет программ «OpenSSL» (для операционных систем UNIX, Linux и Windows).
Этап 6: Согласование параметров защищенного VPN-туннеля или установления безопасной ассоциации SA в сети VPN		
6.1.	Выбрать способ установления безопасной ассоциации SA	1. Автоматический (на основе протокола IKE и его параметров) 2. Ручной (в этом случае системный администратор сети конфигурирует вручную все объекты и субъекты сети VPN)
6.2.	Выбрать протокол защиты переда-ваемых данных	1. Выбрать протокол AH 2. Выбрать протокол ESP 3. Выбрать комбинированное использование протоколов AH и ESP
6.3.	Выбрать алгоритм аутентификации протокола AH и его ключи	1. Протокол AH обязательно должен поддерживать алгоритм HMAC-SHA1-96 2. Желательно, чтобы протокол AH поддерживал алгоритм AES-XCBC-MAC-96 3. Допустимо, чтобы протокол AH поддерживал алгоритм HMAC-MD5-96
6.4.	Выбрать алгоритм шифрования, используемый протоколом ESP, и его ключи	1. Протокол ESP обязательно должен поддерживать следующие алгоритмы (хотя он может использовать один алгоритм для шифрования – DES или NULL – и один алгоритм для аутентификации – HMAC или NULL): алгоритм DES в CBC режиме; алгоритм HMAC совместно с алгоритмом MD5 алгоритм HMAC совместно с алгоритмом SHA-1 алгоритм NULL-аутентификации алгоритм NULL-шифрования

		2. Допустимо отключение процесса аутентификации 3. Допустимо, чтобы протокол ESP использовал один из следующих алгоритмов: AES, 3DES, IDEA, CAST, RC5
6.5.	Выбрать алгоритм аутентификации протокола ESP и его ключи	1. Обязательное использование: протокол ESP обязательно должен использовать один из следующих алгоритмов: алгоритм HMAC совместно с алгоритмом MD5 алгоритм HMAC совместно с алгоритмом SHA-1 2. Допустимое использование: допустимо, чтобы протокол ESP использовал алгоритм NULL-аутентификации
6.7.	Выбрать способы защиты сеанса обмена	Выбрать одну из групп защиты в алгоритме Диффи-Хеллмана: 1. DH группа 1 (768-бит) 2. DH группа 2 (1024-бит) 3. DH группа 5 (1536-бит) 4. DH группа 14 (2048-бит)
6.8.	Выбрать частоту смены ключей	1. Параметры «по умолчанию»: генерировать новый ключ для каждых 100 МБ информации или через каждые 900 секунд 2. Выбрать максимальный объем информации для использования одного и того же ключа (в МБ) 3. Выбрать максимальный отрезок времени для использования одного и того же ключа (в секундах)
Этап 7: Создание цифровых сертификатов всем участникам обмена данными в сети VPN (если в шаге 4.1. выбрано решение на основе цифровой подписи и цифровых сертификатов формата X.509)		
7.1.	Создать цифровые сертификаты на основе выбранной криптосистемы для каждого объекта и субъекта сети VPN	Выполнить следующие последовательные операции: 1. Сгенерировать пару ключей (секретный ключ и открытый ключ), которые являются уникальными для каждого участника обмена данными в сети VPN 2. Каждому участнику создать запрос на сертификат, включая в него информацию о стране, регионе или области, организации, подразделения в компании, имени и электронном адресе участника 3. Пакет программ «Центр сертификации» должен подписать каждый запрос на выдачу сертификата. Возможные опции: длина ключа должна составлять а) 1024 бита (минимальная длина), б) 2048 битов (рекомендуемая длина).
Этап 8: Рабочий (штатный) режим функционирования сети VPN		
8.1.	Установить контакт (hand-shaking) между хостами, находящимся на разных концах VPN-туннеля	При условии выбора решения «цифровой сертификат» на шаге 4.1.: 1. Внутренние хосты (серверы) должны отвечать на запрос внешнего хоста (пользовательского компьютера) о построении IPSec VPN-туннеля (отметим, что внутренние хосты КОС не инициируют процесс туннелирования). 2. Внутренние хосты должны проверять а) подлинность цифрового сертификата каждого обратившегося к ним

		участника (клиента) и б) цифровую подпись, поставленную пакетом программ «Центр сертификации». 3. Внешние хосты (клиенты) должны а) создать IPSec VPN-туннель, б) проверить подлинность сертификата каждого внутреннего хоста, в) цифровую подпись, поставленную пакетом программ «Центр сертификации».
		При условии выбора решения «разделяемый секрет» на шаге 4.1.: Всем внутренним и внешним хостам проверять совпадение «разделяемого секрета» на обоих концах IPSec VPN-туннеля.
		При условии выбора решения «активная директория и система Kerberos» на шаге 4.1.: Проверять легитимность всех внутренних и внешних хостов через систему Kerberos.
8.2.	Осуществлять фильтрацию траффика	Межсетевые экраны должны обеспечить пакетную фильтрацию межсетевого траффика и блокировать (отфильтровывать) соединения любого незарегистрированного объекта или субъекта сети VPN. Межсетевые экраны должны пропускать легитимную информацию и данные в созданных IPSec VPN-туннелях за счет открытия 1. IP-протокола 50 (протокол ESP), 2. IP-протокола 51 (протокол AH), 3. протокола IKE (UDP порт 500), 4. протокола IKE (UDP порт 4500) при наличии NAT между хостами
8.3.	Управление и контроль за всеми достигнутыми соглашениями	В процессе непосредственной работы IPSec VPN-туннеля, протокол IKE должен обеспечивать: - контроль за выполнением всех достигнутых договоренностей по безопасному обмену данными в туннеле, - управление всеми параметрами соединения в IPSec VPN-туннеле, - защиту от некоторых типов атак, - регулярную смену ключей объектов и субъектов сети непосредственно в процессе работы туннеля, - согласовывать алгоритмы шифрования данных и их параметры.
8.4.	Обеспечивать конфиденциальность, целостность, аутентичность передаваемых данных и защиту от повторов для пакетов данных.	При условии выбора решения № 2 (ESP) на шаге 6.2. , протокол инкапсулирующей защиты ESP должен осуществлять: 1. шифрование содержимого каждого IP-пакета (для обеспечения конфиденциальности данных), 2. вычисление дайджеста (для обеспечения целостности и аутентичности данных).
		При условии выбора решения № 1 (AH) на шаге 6.2. , протокол аутентифицирующего заголовка AH должен гарантировать получателю данных в IPSec VNP-туннеле, что: 1. IP-пакет был отправлен легитимным участником сети

		VPN (аутентичность), 2. содержимое пакета осталось неизменным в процессе его передачи через туннель (целостность), 3. пакет не является дубликатом другого пакета, полученного ранее (защита от повторов).
		При условии выбора решения № 3 (AH+ESP) на шаге 6.2. , протоколы AH и ESP работают одновременно и выполняют функции, определенные настройками параметров протокола IKE или указанные вручную системным администратором при конфигурировании системы.

Комбинированная методика СЗИ IPSec VPN с разграничением доступа.

Одним из основных достоинств разработанной и описанной выше методики является тот факт, что она позволяет комбинирование с принципиально разными моделями обеспечения безопасности КОС, например, с моделями ролевого разграничения доступа (РРД).

Задачи, решаемые при создании компьютерных систем, реализующих базовые политики обеспечения безопасности КОС на основе разграничения доступа – дискреционные и мандатные - можно разделить на 3 основные группы.

Обеспечение выполнения пометки субъектов и объектов КОС (т.е. каждому объекту КОС должен быть присвоен уровень конфиденциальности, а каждому субъекту КОС - уровень доступа) и правил мандатного разграничения доступа к объектам КОС.

Определения порядка функционирования доверенных субъектов КОС.

Обеспечение безопасности информационных потоков в КОС.

Как правило, для решения первой перечисленной задачи используют математические модели системы мандатного разграничения доступа и средства присваивания меток доступа объектам и субъектам КОС. Для решения второй задачи – математические модели дискреционного разграничения доступа. Однако, модели мандатного и дискреционного разграничения имеют некоторые недостатки. Более того, они не решают третью указанную проблему [4].

Поэтому, ниже предлагается решение первой и второй задач с использованием модели РРД, а третьей задачи – методами систем защиты на основе IPSec VPN-сетей. Известно, что модели РРД более гибки и эффективны, чем модели мандатного разграничения; они наиболее эффективно работают в компьютерных системах, для пользователей которых четко определен круг 1) их прав доступа на объекты компьютерной системы, 2) типов сессий между пользователями и компьютерными системами, 3) типов ролей пользователей, на которые может быть авторизован пользователь.

Общая идея разработанной методики заключается в следующем.

1. Построить зоны разграничения доступа пользователей по принципу:

а) MZ – зона объектов КОС со строго ограниченным доступом, которые предназначены для хранения строго конфиденциальной информации (например, серверы баз данных со всеми данными об академической успеваемости на-

стоящих и бывших студентов, о заработной платы сотрудников университета, и т.п.); строго ограниченный перечень пользователей и со строго ограниченного списка компьютеров может иметь доступ к объектам этой зоны;
б) AZ - зона объектов КОС со строго ограниченным доступом, которые предназначены для управления работой и безопасностью КОС (например, объекты КОС для системных администраторов); строго ограниченный перечень пользователей и со строго ограниченного списка компьютеров может иметь доступ к объектам этой зоны;
в) DZ – зона объектов КОС с ограниченным доступом, которые предназначены, например, для хранения академического контента, курсов, образовательных модулей, и т.п.; для операции «*изменить информацию*» только ограниченный перечень пользователей может иметь доступ к объектам этой зоны; для операции «*читать информацию*» объекты зоны открыты для легитимных пользователей – студентов и преподавателей университета;
г) WZ – зона объектов КОС с Web-приложениями (например, системы управления электронным образованием Blackboard или Moodle, системы электронной почты, и др.); объекты зоны открыты для всех легитимных пользователей – студентов и преподавателей университета;
д) UZ – зона пользовательских объектов КОС с соответствующими подзонами, такими, например, как учебные компьютерные лаборатории, офисы преподавателей, научно-исследовательские центры и лаборатории, библиотеки, общежития студентов, и т.п.; объекты зоны открыты для всех легитимных пользователей – студентов и преподавателей университета.

2. Построить систему СЗИ-VPN КОС по схеме «внутрикорпоративная сеть VPN » для обеспечения безопасности информационных потоков в КОС от атак извне.

3. С целью обеспечения безопасности информационных потоков в КОС от атак изнутри использовать интегрированное техническое решение на основе программного обеспечения (IPSec VPN) и межсетевых экранов для построения технических VPN-решений для всех зон КОС.

4. Использовать средства систем мандатного разграничения доступа и средства присваивания меток доступа для всех объектов и субъектов КОС.

5. Использовать средства систем дискреционного разграничения доступа для определения порядка функционирования доверенных субъектов КОС. Для этого разбить все субъекты КОС на группы (например, студенты, преподаватели, администраторы верхнего уровня менеджмента, системные администраторы, и т.п.), которые имели бы разные права и роли доступа субъектов к объектам КОС в различных ее зонах.

Методика СЗИ IPSec VPN типа «хост-МЭ-хост» для удаленного пользователя

Другим достоинством разработанной и описанной выше методики является тот факт, что она позволяет комбинирование с другими техническими средствами обеспечения безопасности КОС. Например, при определенных на-

стройках указанная методика в варианте решения № 4 (комбинированное решения) этапа 1 позволяет IPSec VPN-каналу «проходить» через межсетевые экраны; иными словами, для легитимных пользователей и приложений созданной сети VPN установленные межсетевые экраны будут «прозрачными». Общая идея этой методики заключается в том, что на фильтрующем МЭ открывается ограниченное число портов и протоколов: 1) в минимальном варианте: а) протокол 50 (для протокола ESP) и б) UDP порт 500 (для протокола IKE), 2) в максимальном варианте: к минимальному варианту добавляются в) протокол 51 (для протокола AH) и г) UDP порт 4500 для случаев одновременного использования протоколов AH и ESP, а также наличия транслятора IP-адресов NAT между хостами IPSec VPN-туннеля. Таким образом, все информационные потоки, проходящие через МЭ, либо фильтруются средствами самого МЭ, либо должны обладать статусом легитимности, определяемым средствами IPSec VPN-туннеля. В результате, для получения доступа к защищенному серверу КОС, работающим с субъектом КОС только через IPSec VPN-туннель, злоумышленники вынуждены взламывать сам IPSec VPN-туннель. Для этого им необходимо либо обрести подписанный цифровой сертификат подлинности либо определить значение разделяемого секрета, что, в общем случае, означает необходимость взлома криптографических алгоритмов. Эта задача является гораздо более трудоемкой, чем задача взлома открытых сервисов на незащищенных серверах КОС.

СПИСОК ЛИТЕРАТУРЫ:

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008.
2. Сердюк В.А. Новое в защите от взлома корпоративных систем. – М.: Техносфера, 2007.
3. Усков А.В., Иванников А.Д., Усков В.Л. Обобщенная методика построения VPN-решений для систем информационной защиты корпоративных образовательных сетей // Труды V международной научно-методической конференции "Новые образовательные технологии в вузе". – Екатеринбург.: УГТУ-УПИ, 2008. [Данный сборник]
4. Девянин П.Н. Модели безопасности компьютерных систем. – М.: Издательский центр «Академия», 2005.